BUFNETS
BULLETIN OF NETWORK ENGINEERING AND INFORMATICS
https://bufnets.tech

BULLETIN OF NETWORK ENGINEERING AND INFORMATICS
Vol. 1 No 1 – April 2023

ANALISIS TRAFIK ABNORMAL MENGGUNAKAN WIRESHARK (STUDI KASUS: SISTER.UMMETRO.AC.ID)

ABNORMAL TRAFFIC ANALYSIS USING WIRESHARK (CASE STUDY: SISTER.UMMETRO.AC.ID)

Arif Hidayat

Ilmu Komputer, Fakultas Ilmu Komputer, Universitas Muhammadiyah Metro
Jl. Gatot Subroto No.100, Yosodadi Kota Metro Lampung, Indonesia

e-mail: androidarifhidayat@gmail.com

Received : 23 February 2023	Accepted : 24 February 2023	Published : 20 April 2023

Abstract

Information technology that is increasingly developing requires a security mechanism that can guarantee confidentiality, integrity, and availability. one of the existing information technologies within Muhammadiyah Metro University, namely SISTER (Integrated Resource Information System) SISTER is an application that is used to fill in the portfolios of educators in Indonesia. SISTER is installed in each tertiary institution, the SISTER problem for university administrators is that this system does not give root access to university administrators so if there is an abnormality in the application it will make it difficult for administrators to block access from attackers, for this reason, this research will analyze the traffic that is on SISTER and see abnormal activity using the Wireshark tool so that if there is abnormal activity on the SISTER network it can be blocked on the internet network side through the router, this research will also test penetration testing on SISTER using the HPING3 tool to find out whether Wireshark can detect attacks which are conducted. The results of this study are an analysis of abnormal activity at SISTER Muhammadiyah University Metro and anticipating using a firewall, the result is that Wireshark can detect HPING3 attacks and the attacker's IP address can be blocked with a firewall.

Keywords: *Network Security, SISTER Ristekdikti, Metasploit, Wireshark, HPING3*

Abstrak

Teknologi informasi yang semakin berkembang membutuhkan mekanisme keamanan yang dapat menjamin kerahasiaan, integritas, dan ketersediaan. salah satu teknologi informasi yang ada di Universitas Muhammadiyah Metro yaitu SISTER (Integrated Resource Information System) SISTER adalah aplikasi yang digunakan untuk mengisi portofolio tenaga pendidik di Indonesia. SISTER dipasang di setiap perguruan tinggi, permasalahan SISTER bagi pengelola universitas adalah sistem ini tidak memberikan akses root kepada pengelola universitas sehingga jika terjadi penyalahgunaan pada aplikasi akan menyulitkan pengelola untuk memblokir akses dari attacker, untuk itu karena penelitian ini akan menganalisa trafik yang ada pada SISTER dan melihat aktivitas penyalahgunaan menggunakan tool Wireshark sehingga jika terjadi aktivitas penyalahgunaan pada jaringan SISTER dapat di blokir pada sisi jaringan internet melalui router, penelitian ini juga akan menguji penetrasi pengujian pada SISTER menggunakan tool HPING3 untuk mengetahui apakah Wireshark dapat mendeteksi serangan yang dilakukan. Hasil dari penelitian ini adalah analisis aktivitas penyalahgunaan SISTER Universitas Muhammadiyah Metro dan mengantisipasinya menggunakan firewall, hasilnya Wireshark dapat mendeteksi serangan HPING3 dan alamat IP penyerang dapat diblokir dengan firewall.

Kata Kunci: *Keamanan jaringan, SISTER Ristekdikti, Metasploit, Wireshark, HPING3*

All articles published in BUFNETS will be immediately and permanently free for everyone to read and download. Under the CC-BY license

1. PENDAHULUAN

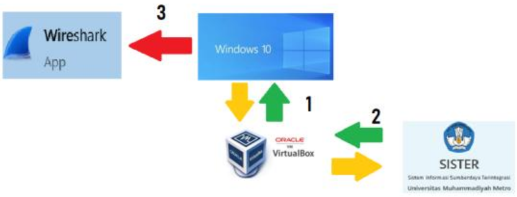
SISTER (Sistem Informasi Sumberdaya Terintegrasi), merupakan aplikasi pelaporan portofolio bagi dosen (tenaga kependidikan), aplikasi ini digunakan untuk melengkapi data dosen yang belum ada pada Pangkalan Data Pendidikan Tinggi (PDDikti) [1]. Aplikasi SISTER digunakan untuk terciptanya integrasi data pada seluruh layanan yang ada pada lingkungan Ristekditki [2]. Mengingat pentingnya fungsi dari aplikasi SISTER maka sangat di perlukan peningkatan keamanan pada SISTER sehingga aplikasi dapat berjalan dengan baik. Aplikasi SISTER yang terpasang pada *server* setiap perguruan tinggi sebagian besar hanya mendapatkan akses *user* bukan *root*, yang menyebabkan tidak terpantaunya aktivitas apa yang terjadi di dalam aplikasi tersebut, ketika ada aktivitas yang tidak semestinya *(abnormal)* pada *server* SISTER administrator perguruan tinggi tidak dapat melakukan apapun karena keterbatasan *privilege* yang di miliki. Beberapa kali *server* SISTER Universitas Muhammadiyah Metro mengalami *down*, hipotesis atau dugaan sementara adalah telah terjadi serangan dari dalam atau luar *server* yang mengganggu kinerja dari aplikasi. Untuk itu di perlukan sebuah *tool* (alat) yang dapat di gunakan untuk memantau trafik mencurigakan dari luar maupun dari dalam *server* SISTER guna mencegahnya pada sisi jaringan internet.

Beberapa serangan yang sering terjadi dan sangat popular adalah serangan *Distributed Denial of Service (DDoS)* yang berakibat terganggunya akses ke *server*, sehingga *availability* data menjadi terganggu [3]. Dalam menganalisis trafik yang ada di dalam jaringan dapat menggunakan *tool* Wireshark dimana *tool* tersebut dapat digunakan untuk *capturing* data yang mengalir pada jaringan[4], data tersebut dapat di manfaatkan untuk di analisis guna menemukan trafik yang tidak normal berdasarkan indikator tertentu[5]. Wireshark memiliki fungsi *filtering* yang dapat digunakan untuk analisis data dengan mudah [6]. Wireshark dapat menangkap (*capturing*) data dan menampilkan data packet jaringan secara detail dan di implementasikan untuk mendeteksi serangan *TCP SYN Flood DDOS* pada jaringan [7].

Berdasarkan pada penelitian sebelumnya yang memanfaatkan Wireshark guna menemukan aktivitas mencurigakan pada sebuah jaringan, maka penelitian ini akan berfokus untuk menganalisis *packet* jaringan yang ada pada *server* SISTER untuk menemukan aktivitas *abnormal* dan melakukan penetrasi *testing* untuk melihat kemampuan yang di miliki Wireshark dalam mendeteksi serangan *DDoS* memanfaatkan *tool* Hping3, hasil dari penelitian ini akan di gunakan untuk meningkatkan keamanan pada jaringan SISTER sehingga aplikasi dapat di akses dengan baik.

2. METODE PENELITIAN

Metode penelitian untuk menemukan perilaku yang tidak normal, untuk menemukan perilaku yang tidak normal pada jaringan dapat dengan menganalisa trafik dari jaringan itu sendiri dengan memanfaatkan Wireshark [8], Berikut ini adalah Gambar 1 yang menunjukan proses capturing packet untuk mendeteksi perilaku abnormal menggunakan Wireshark.



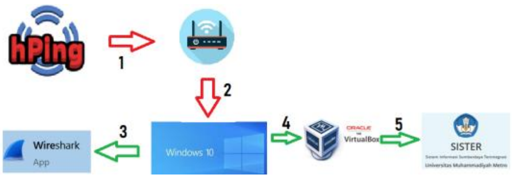
Gambar 1. Eksperimen *capturing packet*

Penjelasan Gambar 1:

a). Pada Gambar 1 yang di tunjukan angka 1 dan 2 merupakan *packet* yang keluar masuk dari jaringan *server* SISTER, SISTER terpasang dengan mekanisme virtualisasi pada Virtualbox yang ada pada sistem operasi induk Windows 10, sehingga packet yang keluar masuk ke SISTER akan melewati *interface* dari sistem operasi Windows 10.

b). Sistem operasi Windows 10 yang menjadi jalur keluar masuk *packet server* SISTER akan di amati dengan menggunakan Wireshark untuk mencari apakah ada aktivitas *abnormal* pada *server*.

Selain melakukan analisis *packet* untuk menemukan aktivitas *abnormal* pada jaringan, penulis akan menguji apakah Wireshark mampu mendeteksi serangan dengan cara melakukan penetrasi *testing* pada *server* SISTER. Berikut ini Gambar 2 yang menunjukan proses penetrasi *testing* yang akan di lakukan.



Gambar 2. Simulasi *penetrasi testing*

Penetrasi *testing* adalah sebuah prosedur yang dilakukan untuk menguji keamanan dari sebuah

All articles published in BUFNETS will be immediately and permanently free for everyone to read and download. Under the CC-BY license

sistem yang telah dibuat dengan cara melakukan simulasi serangan kepada sistem tersebut [9].

Prosedur dalam melakukan penetrasi *testing* pada Gambar 2 akan di jelaskan sebagai berikut:

a). Pada Gambar 2 yang di tunjukan nomor 1 akan di lakukan serangan *TCP SYN Flood* menggunakan *tool* Hping3.

b). Packet yang mengandung serangan akan melalui *router* jaringan dan di teruskan ke *server* SISTER melalui *interface* Windows 10 dan Virtualbox.

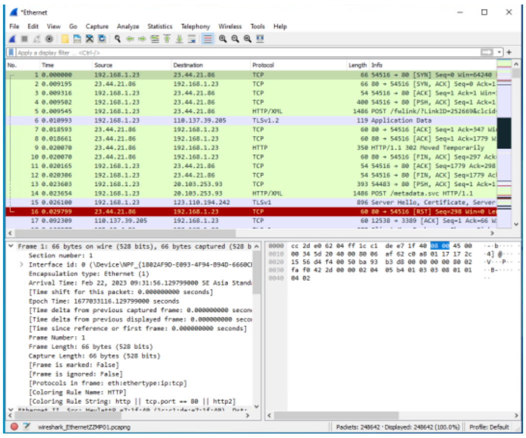
c). Wireshark di pasang untuk menganalisis serangan Hping3.

Dari proses penetrasi *testing* tersebut penulis akan melihat apakah serangan yang di kirimkan Hping3 sesuai dengan *packet* serangan yang ditemukan pada Wireshark sehingga akan terlihat bagaimana kemampuan Wireshark dalam mendeteksi serangan.

3. HASIL DAN PEMBAHASAN

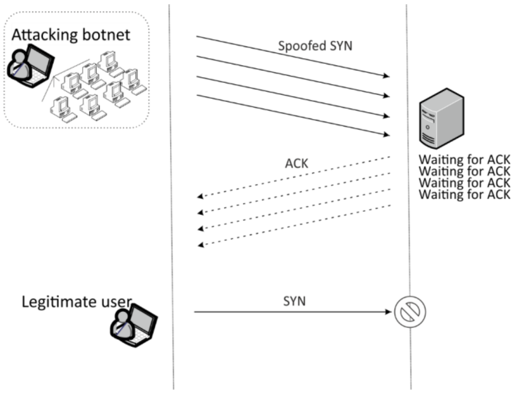
3.1 Analisis *packet* tahap pertama

Analisis *packet* tahap pertama adalah ketika kondisi *server* SISTER berjalan seperti biasanya, artinya *server* berjalan tanpa perlakuan khusus (penetrasi *testing*). Berikut ini Gambar 3 menunjukan proses *capturing packet* yang di lakukan Wireshark pada *interfaces* SISTER.



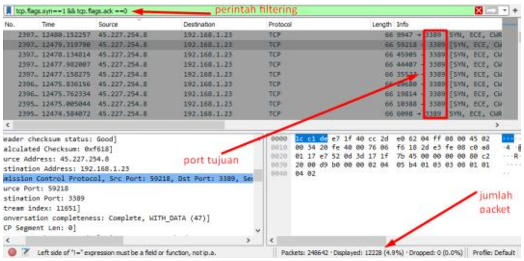
Gambar 3. *Capturing packet* SISTER

Proses *capturing packets* di lakukan selama 3 jam dengan jumlah 248642 *packets*. Dari *packet* tersebut kita akan mencari apakah terdapat serangan *SYN Flood* pada jaringan, Pada kuartal 4 tahun 2021 *SYN Flood* menjadi metode paling banyak di gunakan dalam melakukan serangan [10]. Serangan *SYN Flood* sendiri adalah metode serangan dengan mengeksploitasi *three-way handshaking* yaitu mekanisme terbangunya suatu koneksi antara *client* dan *server*, dimana *attacker* akan mengirimkan *packet SYN* ke *server* sehingga *server* merespon dengan mengirimkan *SYN-ACK packet* ke *attacker*, *server* akan menunggu packet *ACK* dari *attacker* yang tidak pernah di kirimkan kembali ke *server*, konsekuensinya *resource server* terpakai untuk menunggu *packet ACK* tersebut sehingga *server* sibuk dan tidak akan dapat melayani pengguna lain [11]. berikut ini merupakan Gambar 4 yang menunjukan proses serangan *SYN Flood*.



Gambar 4. Serangan *SYN Flood*
[Sumber: Huraj, L., Šimon, M., & Horák, T. (2020)]

Dengan mengetahui mekanisme serangan *SYN Flood* maka hal yang di lakukan adalah dengan melakukan *filtering* pada Wireshark dengan menggukan perintah “tcp.flags.syn==1 && tcp.flags.ack ==0” dimana perintah tersebut akan melakukan *filtering packet* yang memiliki *TCP flag SYN* namun tidak memiliki *TCP flag ACK*. Berikut ini adalah Gambar 5 yang menunjukan hasil *filtering packet* yang di lakukan.



Gambar 5. *Filtering packet SYN*

Dari Gambar 5 terdapat 12228 *packets* yang di tampilkan atau sekitar 4.9% *packet* yang masuk dalam kategori serangan *SYN Flood*. Gambar 5 juga menunjukan bahwa *packet* di tujukan ke *port* 3389 dimana *server* SISTER tidak menjalankan *service* pada *port* 3389 (*Remote Desktop Protocol*), sehingga sangat tidak wajar apabila terdapat *IP Addresses* dari Negara yang tidak relevan mengakses SISTER pada *port* yang tidak di gunakan dengan jumlah *packet* yang sangat tinggi. Statistik IP Addresses yang

All articles published in BUFNETS will be immediately and permanently free for everyone to read and download. Under the CC-BY license

melakukan *SYN Flood* dapat di tampilkan dengan menggunakan menu statistik yang ada pada Wireshark. Berikut ini Gambar 6 yang menunjukan statistik 5 Besar *IP Addresses* yang melakukan *SYN Flood*.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent
Source IPv4 Addresses	11090				0.0009	100%
194.165.16.78	794				0.0001	7.16%
45.227.254.8	772				0.0001	6.96%
194.165.16.76	772				0.0001	6.96%
194.165.16.77	697				0.0001	6.28%
194.165.16.73	681				0.0001	6.14%

Gambar 6. Statistik *SYN Flood*

Dari 11090 *packets* 5 *IP Addresses* tersebut menyumbang sekitar 33,5% dari total *packets* 161 *IP Address*.

3.2 Analisis *packet* tahap penetrasi *testing*

Analisis *packet* pada saat terjadinya penetrasi *testing*, *packet* ini akan di amati guna melihat akurasi Wireshark dalam mendeteksi *tool* Hping3 yang dapat di gunakan untuk melakukan serangan *SYN Flood* [12],[13],[14],[15]. Proses penetrasi testing di lakukan dengan mencatat IP Address attacker, IP Address attacker di tunjukan pada Gambar 7 di bawah ini.

Gambar 7. IP Address attacker

Setelah mencatat *IP Address attacker*, proses selanjutnya adalah menjalankan Wireshark pada sistem operasi induk Windows 10. Setelah Wireshark di jalankan, proses serangan menggunakan *tool* Hping3. Berikut Gambar 8 yang menunjukan proses serangan menggunakan Hping3.

```
└─# hping3 -S sister.ummetro.ac.id -p 80
HPING sister.ummetro.ac.id (eth0 103.213.116.82): S set, 40 headers + 0 data bytes
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=47.9 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=1 win=29200 rtt=31.3 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=2 win=29200 rtt=70.5 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=3 win=29200 rtt=38.5 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=4 win=29200 rtt=53.7 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=5 win=29200 rtt=24.7 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=6 win=29200 rtt=27.3 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=7 win=29200 rtt=42.6 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=8 win=29200 rtt=50.7 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=21 win=29200 rtt=841.2 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=22 win=29200 rtt=38.0 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=23 win=29200 rtt=49.1 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=24 win=29200 rtt=57.0 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=25 win=29200 rtt=47.8 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=26 win=29200 rtt=44.8 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=27 win=29200 rtt=25.4 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=28 win=29200 rtt=47.7 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=29 win=29200 rtt=47.8 ms
len=46 ip=103.213.116.82 ttl=56 DF id=0 sport=80 flags=SA seq=30 win=29200 rtt=38.8 ms
^C
--- sister.ummetro.ac.id hping statistic ---
77 packets transmitted, 19 packets received, 76% packet loss
round-trip min/avg/max = 24.7/85.5/841.2 ms
```

Gambar 8. Hping3 Attack

Penjelasan Gambar 8.

a). Perintah yang di lakukan pada *tool* Hping 3 yaitu "hping3 –S sister.ummetro.ac.id –p 80".
b). hping3 digunakan untuk menjalankan *tool* hping3.
c). –S untuk mengirimkan packet *SYN*.
d). sister.ummetro.ac.id merupakan *target* yang akan di serang.
e). –p 80 digunakan untuk mengirimkan *packet* ke *port* 80.

Dari proses serangan menggunakan Hping3, serangan tersebut mengirimkan 19 *packets* ke *target*. Wireshark berhasil mendeteksi serangan tersebut, berikut ini Gambar 9 yang menunjukan statistik serangan *SYN Flood* yang terdeteksi Wireshark.

Wireshark · Source and Destination Addresses · Ethernet

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Source IPv4 Addresses	41				0.0004	100%	0.0100	0.973
110.137.38.190	19				0.0002	46.34%	0.0100	1.141

Gambar 9. Statistik penetrasi *testing* pada Wireshark

Hasil dari statistik Wireshark memiliki akurasi 100% dengan serangan yang di lakukan Hping3, serangan Hping3 memiliki jumlah yang sama dengan serangan yang di deteksi Wireshark yaitu sebanyak 19 serangan.

4. KESIMPULAN

Hasil analisis tahap pertama menunjukan bahwa dugaan adanya serangan pada *server* sister.ummetro.ac.id yang menggangu kinerja dari *server* benar, hal tersebut di tunjukan pada Gambar 5 yaitu terdapat 12228 *packets* (4,9%) dari keseluruhan *packets* yang melakukan *SYN Flood attack* pada *server*, serangan di tujukan ke port 3389 yaitu *port remote desktop protocol*, server SISTER sendiri tidak menggunakan *port* tersebut dan jarang sekali di akses dari luar indonesia.

Analisis *packet* pada saat penetrasi *testing* menunjukan bahwa Wireshark mampu mendeteksi serangan yang di kirim oleh Hping3, *packet SYN* yang terdeteksi pada Wireshark sama dengan *packet SYN* yang di kirimkan Hping3, artinya Wireshark memiliki ke akuratan sebesar 100% di dalam mendeteksi serangan *SYN Flood*.

PERNYATAAN PENGHARGAAN

Penulis mengucapkan pada semua penulis yang di kutip pada tulisan ini, secara tidak langsung tulisan yang di kutip sangat membantu di dalam menyelesaikan tulisan ini. Tidak lupa ucapan terimakasih sebesar-besarnya kepada Universitas Muhammadiyah Metro yang telah memberikan kesempatan dan wewenang untuk melakukan uji coba pada server sister.ummetro.ac.id.

All articles published in BUFNETS will be immediately and permanently free for everyone to read and download. Under the CC-BY license

DAFTAR PUSTAKA

[1] Harjono, L. A., Santoso, L. W., Andjarwirawan, J., & Lim, R. (2020). Implementasi Web Service Integrasi Data Penelitian dan Pengabdian Masyarakat dengan SISTER Ristekdikti dengan Metode REST. Jurnal Infra, 8(2), 12-18.

[2] TB, D. R. Y., & Aulia, N. (2022). SOSIALISASI TEKNIS PENGISIAN APLIKASI SISTER BAGI DOSEN DAN CIVITAS AKADEMIKA UNIVERSITAS UBUDIYAH INDONESIA. JURNAL PENGABDIAN KEPADA MASYARAKAT INOTEC UUI, 4(1), 11-16.

[3] Ali, M. H., Jaber, M. M., Abd, S. K., Rehman, A., Awan, M. J., Damaševičius, R., & Bahaj, S. A. (2022). Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT). Electronics, 11(3), 494.

[4] Mabsali, N. A., Jassim, H., & Mani, J. (2023, January). Effectiveness of Wireshark Tool for Detecting Attacks and Vulnerabilities in Network Traffic. In 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022) (pp. 114-135). Atlantis Press.

[5] Dodiya, B., & Singh, U. (2022). Malicious traffic analysis using Wireshark by collection of indicators of compromise. Int J Comput Appl, 183, 975-8887.

[6] Wijaya, R., & Hidayat, R. (2022). ANALYSIS OF PREVENTION OF ILLEGAL ACTIVITIES ON THE NETWORK. JOURNAL OF DYNAMICS (International Journal of Dynamics in Engineering and Sciences), 17(2), 153-156.

[7] Rana, D. S., Garg, N., & Chamoli, S. K. (2012). A Study and Detection of TCP *SYN* Flood Attacks with IP spoofing and its Mitigations. International Journal of Computer Technology and Applications, 3(4), 1476-1480.

[8] Saputra, I. P., Utami, E., & Muhammad, A. H. (2022, October). Comparison of anomaly based and signature based methods in detection of scanning vulnerability. In 2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (pp. 221-225). IEEE.

[9] Hidayat, A., & Saputra, I. P. (2018). Analisa Dan Problem Solving Keamanan Router Mikrotik Rb750Ra Dan Rb750Gr3 Dengan Metode Penetration Testing (Studi Kasus: Warnet Aulia. Net, Tanjung Harapan Lampung Timur). Jurnal RESISTOR (Rekayasa Sistem Komputer), 1(2), 118-124.

[10] European Union Agency for Cybersecurity (EU body or agency), 2022, pp. 75–76.

[11] Huraj, L., Šimon, M., & Horák, T. (2020). Resistance of IoT sensors against DDoS attack in smart home environment. *Sensors*, *20*(18), 5298.

[12] Adams, D. (1969, August 01). Retrieved February 23, 2023, from https://linuxhint.com/hping3/.

[13] Ahda, A., Wulandari, C., Husellvi, H. P., Alhuda, M. Y., Reda, M., Zahwa, P., & Ananda, S. (2023). INFORMATION SECURITY IMPLEMENTATION OF DDOS ATTACK USING HPING3 TOOLS. *JComce-Journal of Computer Science*, *1*(4).

[14] Tampati, I. F., Setyawan, F. G., Sejati, W. W., & Kardian, A. R. Comparative Analysis of CPU Performance on FreeBSD 64-bit and RedHat 64-bit Operating System Against Denial of Service (DoS) Using Hping3. CESS (Journal of Computer Engineering, System and Science), 8(1), 209-219.

[15] Alzahrani, A. O., & Alenazi, M. J. (2023). ML-IDSDN: Machine learning based intrusion detection system for software-defined network. Concurrency and Computation: Practice and Experience, 35(1), e7438.

All articles published in BUFNETS will be immediately and permanently free for everyone to read and download. Under the CC-BY license